El cibercrimen, un delito económico en alza

Toni Martínez

Miembro del Colegio Oficial de Ingenieros de Telecomunicación de la Comunidad Valenciana. CTO de Bee Ingeniería

El aumento del cibercrimen, que supone ya un 32 por ciento del total de delitos económicos en España -según datos del Instituto Nacional de Ciberseguridad-, está perjudicando seriamente a empresas y ciudadanos. Estos datos son el resultado de la transformación digital y el Internet de las cosas (IoT), que están cambiando drásticamente el paradigma de la información y están dando entrada a criminales cibernéticos que no solo buscan acceder a información sensible, sino ser los protagonistas en alguno de los procesos más determinantes de nuestra sociedad.

Si bien inicialmente el perfil de estos atacantes parecía ser el de un hacker con pinta de *friki* y pocas habilidades sociales, encerrado a oscuras en su habitación intentando buscar algún agujero de seguridad, el de hoy no tiene nada que ver. El cibercrimen se ha profesionalizado, dando lugar a poderosos grupos formados por talentosos profesionales capaces de diseñar las más complicadas estrategias para dar al traste con casi cualquier sistema digital que uno pudiera imaginar. Son grupos organizados y sofisticados.

A este cambio radical en el concepto de hacker, hay que unir dos grandes evoluciones en la sociedad que han provocado un importante cambio en el paradigma del cibercrimen: la transformación digital y el Internet de las cosas.

La primera de ellas nos ha ayudado a optimizar y hacer más eficientes muchos de los procesos de nuestro día a día, pero también ha provocado que situaciones que no requerían atención en el aspecto de la ciberseguridad -como, por ejemplo, los vehículos conectados o los controles de acceso- sean ahora el principal objetivo de muchas de esas organizaciones criminales.

Hemos tenido varios casos recientemente en los que se ha abierto la posibilidad de que el cibercrimen actuara en situaciones de un impacto social incalculable. Sin duda, la que más ha llamado la atención es la posible participación de un grupo de hackers rusos en los resultados de las elecciones de Estados Unidos. Y no sólo hablamos de elecciones, sino de referéndums, como podrían ser el del *Brexit* o la autodeterminación en España. ¿Qué pasaría si un grupo cibercriminal pudiera influir en esos resultados?

De momento, tal es la alarma generada al respecto que Holanda ha decidido llevar a cabo el recuento de los votos de sus elecciones de manera tradicional -manualmente-, de cara a evitar posibles ataques por parte de cualquier hacker.

El cibercrimen se ha profesionalizado, con poderosos grupos de talentosos profesionales capaces de diseñar las más complicadas estrategias para dar al traste con casi cualquier sistema digital que uno pudiera imaginar

Pero no solo los procesos electorales están bajo este tipo de amenazas. Sin ir más lejos, hace unas semanas los clientes de un hotel se quedaron encerrados en sus habitaciones por culpa de un ataque cibernético.

Lo que queda a las claras es que la transformación digital obliga a las organizaciones a elevar notablemente su nivel de cuidado a la hora de diseñar soluciones de ciberseguridad, ya que la información que puede quedar expuesta es sumamente sensible para sus intereses.

Y si la transformación digital obliga a ello lo mismo podríamos decir del *IoT*, un concepto que engloba la capacidad de que nuestros objetos cotidianos estén interconectados. El *IoT* abandera una nueva revolución, que muchos comparan con la revolución industrial, pero debemos ser conscientes de que no sólo abrimos una puerta hacia un futuro sin límites, sino también a multiplicar por millones las puertas de entrada a esas mentes que ponen su talento del lado del mal.

Sin ir más lejos, en octubre el dispositivo *zombi* Mirai estuvo cerca de dejar al mundo entero sin Internet haciendo uso de dispositivos tan *inofensivos* como cámaras, codificadores o *routers* como los que cualquiera puede tener en casa.

Lógicamente, estos niveles de alarma no deben provocar un miedo incontenible a navegar por la red o a compartir ficheros con nuestros seres queridos, pero sí que nos debe hacer ver que la realidad ha cambiado radicalmente.

Tenemos que pensar que organizaciones tan preparadas y protegidas como Yahoo, Google o el Banco Central Europeo han sufrido recientemente ataques en los que han perdido información sensible de sus clientes.

Esto debe invitarnos a la reflexión y a darnos cuenta de que en muchas ocasiones la tranquilidad en este ámbito no reside tanto en lo protegidos que estamos -tenemos que intentar estarlo-, sino en lo interesante que podamos resultar para una de estas organizaciones criminales de las que hablábamos anteriormente. Por mucho que hagamos, si a alguno de ellos se le mete entre ceja y ceja hacerse con algo que esté en nuestro poder, más tarde o más temprano podrá conseguirlo.

De lo que no hay duda es de que en el ámbito empresarial hay mucho margen de mejora en términos de ciberseguridad. El cibercrimen es una amenaza que ha costado a las empresas de todo el mundo más de 380 billones de dólares, cinco veces más de lo que toda la industria de la ciberseguridad ha sido capaz de generar.

Estos datos se entienden mejor cuando se analiza en detalle el comportamiento de los usuarios. Según el informe *Security Report 2016* de Checkpoint, cada 5 segundos se produce un acceso a una web maliciosa, cada 4 minutos se emplea una aplicación de alto riesgo y cada 32 minutos información sensible está siendo compartida fuera de la organización.

Las empresas parecen haber comenzado a sensibilizarse con este riesgo creciente y están adoptando estrategias de ciberseguridad desde la base, la concienciación de los usuarios, que sin quererlo se convierten, frecuentemente, en los aliados de esos hackers ávidos por información de interés.

Como bien dijo el consejero delegado de Telefónica, José María Álvarez Pallete, “los datos son el petróleo del siglo XXI”, y ya sabemos lo que los seres humanos hemos sido capaces de hacer por el petróleo en el pasado.

Toni Martínez

Miembro del Colegio Oficial de Ingenieros de Telecomunicación de la Comunidad Valenciana.
CTO de Bee Ingeniería

Las empresas han comenzado a sensibilizarse con este riesgo y a adoptar estrategias desde la base, la concienciación del usuario, que sin quererlo se convierte, frecuentemente, en aliados de esos hackers ávidos por información